# Exhibit H

**IN THE SUPERIOR COURT FOR THE DISTRICT OF COLUMBIA**
**CIVIL DIVISION**

| | | |
|---|---|---|
| DISTRICT OF COLUMBIA, | ) | |
| | ) | |
| Plaintiff, | ) | Civil Action No. 2018-CA-008715-B |
| | ) | Judge Maurice A. Ross |
| v. | ) | |
| | ) | |
| FACEBOOK, INC., | ) | |
| | ) | |
| Defendant. | ) | |

**ORDER GRANTING FACEBOOK, INC.'S MOTION FOR SUMMARY JUDGMENT**

## Introduction

On December 19, 2018, the District of Columbia filed a one-count Complaint against Facebook, Inc. based upon alleged misrepresentations regarding protections of user data. The District specifically points to Facebook's alleged lax oversight and enforcement of third-party applications as violations of the District of Columbia Consumer Protection Procedures Act ("CPPA"). D.C. Code §§ 28-3901, *et seq*. On May 17, 2022, Facebook, Inc. filed a Motion for Summary Judgment. After extensive briefing by the parties, a Motion Hearing was held before the Court on March 21, 2023. The matter is now ripe for resolution.

## Background

Launched in 2004, Facebook is a social networking service that operates a website (Facebook.com) and companion mobile applications ("application" and "app" are terms used interchangeably). Facebook boasts roughly two billion active users. The main utility of the service is to allow users to connect and communicate with other users. Facebook users can add other users as "friends," follow or like pages, create or join groups, and interact with third-party applications. When joining Facebook, users expressly agreed to the Statement of Rights and

Responsibilities ("SRR"), now known as the Terms of Service, and the Data Use Policy which set out the policies. These policies described the Facebook platform and informed users of how their information is shared. Users were able to change their settings to determine what information and data of their profile could be shared.

**Third-Party Applications and Friend-Sharing**

During the relevant time period, users could install third-party applications on Facebook. These third-party applications created additional user experiences on Facebook, such as games, news, music services, birthday reminders, and pop culture and personality quizzes. These third-party applications had various terms of service that dictated what information was shared from Facebook to the third-party application. For example, if a user played a word-search game, that game application may ask for access to the user's friend list so that users could play the game with their friends. This information sharing would only be allowed if the user's settings allowed for it and the user accepted the various terms of service of the application.[1]

**Integration Partnerships**

Facebook also utilized "integration partnerships" until roughly December 2018. Facebook SUMF 268. Integration partnerships allowed device manufacturers and operating systems to create apps which replicated Facebook or the Facebook experience on users' devices. Facebook SUMF 245-258. For example, an integration partnership with BlackBerry allowed BlackBerry to make a Facebook application. *Id.* Notably, Android and iOS had not yet become the predominant method of accessing internet and applications. Facebook SUMF 248. Instead, integration partnerships with companies such as Apple, Amazon, Blackberry, and Yahoo were

[1] During a portion of this time, November 2018 through April 2018, the practice of friend-sharing was active. Friend-sharing allowed users to share certain information about their friends if both the user's and the friends' settings allowed for it. For example, sharing a user's friend list with a game as stated above.

used to build Facebook apps or platforms for each specific device, which was the norm at the time. Facebook SUMF 248-250. Users had to opt into these integration partnerships affirmatively by granting permission, for example by downloading the app and agreeing to the terms. Facebook SUMF 253, 261.

**Enforcement Program**

The enforcement program was a tool outlined by Facebook which included monitoring for potential violations of Facebook's policies, confirmation that a violation occurred, a determination of the appropriate enforcement action in response to a violation, and execution of the determined enforcement action. Facebook SUMF 270. Facebook used a range of measures to monitor third-party apps and ensure compliance, including both manual review and automated review. Facebook SUMF 272-273. Automated review utilized a variety of programs that attempted to detect any kind of signals that would warrant human review, such as rapid app growth, app seeking obviously unnecessary information, users deleting content by the app poster to their timelines, a high number of app uninstalls, and a high call volume. Facebook SUMF 288-289. Once a policy violation had been discovered, Facebook could take a range of enforcement actions, including suspension of apps and developers. Facebook SUMF 274.

**Aleksandr Kogan and Cambridge Analytica**

In November 2013, Aleksandr Kogan created a personality quiz app which supported friend-sharing. Facebook SUMF 361. Kogan obtained data from approximately 300,000 users who installed this app, as well as data from those users' friends in instances where the user gave permission and the friends' privacy settings allowed it. Facebook SUMF 356-360, 378-385. Kogan sold some of this data to political advertising firm Cambridge Analytica. *Id.* Facebook became aware of this incident after an article was published in December 2015. Facebook SUMF

356-360, 378-385. In response, Facebook removed Kogan's app, demanded Kogan delete the user data in his possession, and began an investigation. Both Kogan and Cambridge Analytica provided written certifications that all of the data had been accounted for and destroyed. Facebook SUMF 387-391. In March 2018, Facebook learned from media inquiries that Cambridge Analytica may not have destroyed the data and may have used it for political advertising, contrary to its prior representations. Facebook SUMF 392. In response, Facebook banned Cambridge Analytica and initiated an investigation. Facebook SUMF 393-394. Also, Facebook notified users who may have been affected beginning on April 9, 2018. Facebook SUMF 397-404. The notice was in the form of a dialog box upon logging into the platform. There were three potential messages presented to the user, depending on whether that user had been impacted. *Id.*

**Legal Action**

In December 2018, the District brought a one-count Complaint against Facebook alleging violations of the CPPA by making misleading representations, misleading omissions, and misleading ambiguous statements. The core theory of the District's case revolved around how user information could be shared with third-party apps. The District contends that Facebook failed to honor its promise to protect user data, instead exerting lax oversight and enforcement of third-party applications. Specifically, the misleading disclosures fell into five categories: (1) friend-sharing, (2) integration partnerships, (3) enforcement, (4) privacy settings, and (5) data-misuse disclosures, specifically involving Cambridge Analytica.

On May 17, 2022, Facebook, Inc. filed a Motion for Summary Judgment. Facebook's theory of the case is that after years of discovery, the District has failed to produce any evidence of what exactly misled consumers. Facebook points to three other cases where the Court has

considered, and rejected, this very theory challenging Facebook's disclosures.[2] Facebook further asserts that the District has failed to produce any evidence as to what differentiates this claim from every other case before it. Facebook asks for summary judgment because Facebook repeatedly and accurately disclosed their policies to consumers. Thus, with accurate and thorough disclosures, a consumer could not have been misled about Facebook's policies.

**Legal Standard**

To prevail on a motion for summary judgment, the moving party has the burden of demonstrating based on the pleadings, discovery, and any affidavits submitted, that there is no genuine issue as to any material fact. Super. Ct. Civ. R. 56(c); *Wash. Inv. Ptnrs. Of Del., LTC v. Sec. House*, 28 A.3d 566, 573 (D.C. 2011); *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). "A genuine issue of material fact existed if the record contains 'some significant probative evidence…so that a reasonable fact-finder would return a verdict for the non-moving party." *Brown v. 1301 K St. Ltd. P'ship*, 31 A.3d 902, 908 (D.C. 2011).

In ruling on a motion for summary judgment, the evidence must be viewed in the light most favorable to the party opposing the motion. *Rustin v. District of Columbia*, 491 A.2d 496, 500 n.7, *cert denied* (1985). The Court cannot "resolve issues of fact or weigh evidence at the summary judgment stage." *Barrett v. Covington & Burling, LLP*, 979 A.2d 1239, 1244 (D.C. 2009). "A movant is entitled to summary judgment when the evidence is such that a reasonable jury, drawing all reasonable inferences in the non-movant's favor, could not return a verdict for the non-movant." *See Walker v. Johnson*, 798 F.3d 1085, 1091 (D.C. Cir. 2015) (*citing Anderson*

[2] *See In re Facebook, Inc. Sec. Litig.*, 405 F. Supp. 3d 809, 846 (N.D. Cal. 2019) (dismissing claim because Facebook user agreements included third-party consent and were not inaccurate or misleading); *Illinois v. Facebook, Inc.*, No. 2018-CH-03868 (Ill. Cir. Ct. Cook Cnty. Mar. 8, 2021) (rejecting the allegation that a reasonable person reading Facebook policies might believe that their data was guaranteed to be safe from third parties); *Smith v. Facebook, Inc*, 745 F. App'x 8, 8-9 (9th Cir. 2018) (holding that a reasonable person reading Facebook's policies would understand that Facebook uses the practices described in those policies).

*v. Liberty Lobby Inc.*, 477 U.S. 242, 248, 255 (1986). While inferences are drawn in favor of the non-moving party at this stage, "once the moving party has carried its initial burden . . . [t]he party opposing the motion for summary judgment must offer 'competent evidence admissible at trial showing that there is a genuine issue as to a material fact.'" *Hamilton v. Howard Univ.*, 960 A.2d 308, 317-18 (D.C. 2008) (quoting *Sanchez v. Magafan*, 892 A.2d 1130, 1132 (D.C. 2006)).

In order for Facebook to prevail on this summary judgment motion, Facebook must show that there is no genuine issue of material fact and that Facebook is entitled to judgment as a matter of law. The evidence must be viewed in the light most favorable to the non-moving party, and all reasonable inferences must be drawn in that party's favor. The correct evidentiary standard for a CPPA claim is clear and convincing evidence. *See Frankeny v. Dist. Hosp. Partners*, LP, 225 A.3d 999, 1005 (D.C. 2020).[3]

**Statutory Framework**

This action is brought under the CPPA, which protects DC consumers from unfair or deceptive trade practices. D.C. Code §§ 28-3901, et seq. To prevail on a CPPA claim, the District must prove that Facebook made representations, omissions, or ambiguous statements that "have a tendency to mislead" consumers about a "material fact." D.C. Code § 28-3904. In order to successfully plead a CPPA claim, both elements must be met; (1) tendency to mislead, and (2) material fact.

According to the CPPA, a violation occurs regardless of "whether or not any consumer is in fact misled, deceived or damaged thereby." D.C. Code § 28-3904. The representation or misrepresentation is evaluated in the eyes of a reasonable D.C. consumer. The fact that a reasonable consumer could be reasonably misled is sufficient to constitute a violation. *Frankeny*

[3] "The burden of proof for CPPA claims is clear and convincing evidence." Pearson v. Chung, 961 A.2d 1067, 1073 (D.C. 2008).

*v. District Hospital Partners*, LP, 225 A.3d 999 at 1004-1005 (D.C. 2020). A "reasonable consumer generally would not deem an accurate statement to be misleading." *Saucier v. Countrywide Home Loans*, 64 A.3d 428, 442 (D.C. 2013). Statements are not actionable if they are "in fact either accurate, not misleading to a reasonable consumer, or mere puffery." *Whiting v. AARP*, 701 F. Supp. 2d 21, 29 (D.D.C. 2010), *aff'd*, 637 F.3d 355 (D.C. Circ. 2011). Additionally, the misrepresentation need not be done intentionally by Defendant. *Frankeny v. District Hospital Partners*, LP, 225 A.3d 999 at 1004-1005 (D.C. 2020). A fact is material "if a significant number of unsophisticated consumers would find that information important in determining a course of action." *Saucier*, 64 A.3d at 442. Summary judgment is appropriate when "the plaintiff has failed to direct the Court to the existence of any facts from which a reasonable jury could find that the alleged statements or omissions were material in nature." *Id.*

## Analysis

### I. Facebook clearly disclosed all relevant terms in its policies such that a reasonable consumer could not have been misled as a matter of law.

The District alleges that multiple Facebook policies and practices, including friend sharing, integration partnerships, the enforcement program, and privacy settings, are misleading representations, omissions, or ambiguous statements under the CPPA. Looking at the various terms of service and agreements, it is clear that this was not the case. Facebook clearly and repeatedly made disclosures to users about its policies such that the reasonable user could not have been misled as a matter of law. This analysis does not reach the materiality element because a reasonable consumer could not have been misled, materially or not, with the accurate disclosures by Facebook.

### A. Friend-Sharing

The District alleges that Facebook misled consumers about the ability of third-party apps to access users' friends' data, the practice of friend-sharing.[4] Specifically, the District contends that disclosures made by Facebook were (1) ambiguous, misleading, and deceptive because they were hidden in two lengthy documents that users must agree to in order to create a Facebook account, and (2) the consumer controls to change these settings were confusing. On the other hand, Facebook asserts that friend-sharing was disclosed repeatedly and prominently on multiple locations on the website.

The most straightforward disclosure of friend-sharing could be found in the Data Use Policy (effective from December 11, 2012 until January 30, 2015). Facebook SUMF 110. The policy included a section titled "Controlling what is shared when the people you share with use applications" which stated,

> Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Facebook SUMF 110. The Data Use Policy further stated the following:

> Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of the application, your friend would want to give the application her friend list – which includes your User ID – so the applications knows which of her friends is also using it. Your friend might also want to share the music you 'like' on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just friends, the application could ask your friend for permission to share them.

Facebook SUMF 111.

[4] See page 2 for more background on the practice of "friend-sharing."

> *Choosing to make your information public is exactly what it sounds like: anyone, including people off of Facebook, will be able to see it. Choosing to make your information also means that this information: can be associated with you* (i.e. you name, profile pictures, cover photos, timeline, User ID, username, etc) even off Facebook; can show up when someone does a search on Facebook or on a public search engine; *will be accessible to Facebook-integrated games, applications, and websites you and your friends use; and will be accessible to anyone who uses our APIs such as Graph API.*

Facebook SUMF 112 (emphasis added).

> If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means you will no longer be able to use any third-party Facebook integrated games, applications or websites.

Facebook SUMF 115.

Facebook also maintained an App Settings page in the Privacy Settings where users could restrict their data as they so choose. Facebook SUMF 139-153. A consumer could specifically select what kinds of information other Facebook users can view, including all Facebook consumers (most expansive), only Facebook friends (the less expansive default), and a customized list of Facebook friends (the least expansive). Facebook SUMF 139-153. Within the Privacy Settings page, a disclaimer stated, "*the people you share with can always share your information with others, including apps*." Facebook SUMF 153 (emphasis added).

Repeatedly, Facebook disclosed the sharing of this data and pointed users to the applicable settings to turn off the friend-sharing functions. The statements throughout the policies and within the settings were *accurate*. The District has not pointed to any specific language within the policies which is inaccurate. As "reasonable consumer[s] generally would not deem an accurate statement to be misleading," Facebook users could not reasonably be misled by the clear and explicit disclosures of friend-sharing. *Saucier v. Countrywide Home Loans*, 64 A.3d 428, 442 (D.C. 2013) (holding that a "reasonable consumer generally would not

deem an accurate statement to be misleading"). In the United States District Court for the Northern District of California, the Court agreed. There, the Court held that terms agreed to by Facebook users included "allowing the Aleksandr Kogans of the world to interact with users and obtain information of the users' friends through these interactions." *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 792(N.D. Cal. 2019). The District has not plausibly pled that the practice of friend-sharing constitutes a valid CPPA claim because it was accurately disclosed to users.

**B. Integration Partnerships**

The District alleges that consumers had little or no control over whether to permit the sharing of their information with integration partners.[5] The District asserts that Facebook's failure to inform consumers that it permitted certain companies this type of access has a tendency to mislead consumers about a material fact. Facebook's response is twofold; (1) users had to opt into the integration partnerships, and (2) the existence of integrations partnerships was well-known and widely reported.

Integration partners were required, via their terms of service with Facebook, to provide notice to the user about what data they were collecting and how they were going to use that information. Facebook SUMF 260. Also, integration partners could not integrate the user's Facebook features with their device or app without the user's express permission. Facebook SUMF 261. This permission or authorization would be granted by the user by signing into their Facebook account on the device or app and agreeing to the terms. Facebook SUMF 261, 263, 264-265.

Facebook users were given explicit and accurate notice of the integration partners twice. The first notice was given when users began their Facebook experience via the terms of service,

[5] See page 2-3 for more background on the practice of "integration partnerships."

the text of which varied by the partner. Facebook SUMF 264-265. The second notice was given to users in Facebook's Data Use Policy, which outlined the sharing of user information with service providers. Facebook SUMF 265. The Data Use Policy section titled "Apps, websites and other third-party integrations on our using [sic] our Services" stated:

> When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook Friends or use the Facebook Comment or Share button on a website, the game developer or website might get information about your activities in the game or receive a comment or link that you share from their website on Facebook. *In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.*

Facebook SUMF 108 (emphasis added).

With disclosures in the Facebook Data Use Policy and the terms of service, which a user had to affirmatively agree to when using a Facebook experience with an integration partner, the user had been notified twice of the existence and terms of the integration partnership. Any user with two accurate and clear notices could not be materially misled about the existence and operation of the integration partnerships as a matter of law. The accurate disclosures of the integration partnership policies make it impossible for the District to plausibly plead that Facebook made misleading representation or omissions.

### C. Enforcement Program

The District alleges that Facebook's enforcement efforts[6] against third party applications who violated Facebook policies did not live up to the enforcement policies outlined in the Data Use Policy and SRR. Specifically, the District contends that Facebook failed to exert meaningful review or compliance mechanisms to enforce its policies, including the ability to audit third-

[6] See page 3 for more background on the "enforcement program."

party apps. In response, Facebook asserts (1) the District has not proven that Facebook's enforcement and monitoring efforts were insufficient, and (2) even if the District did prove that Facebook's efforts were insufficient, the District has failed to show a misleading discrepancy between Facebook's representations and its enforcement program sufficient for a CPPA claim.

Once again, Facebook was clear in its disclosures and policies about the limitations of the enforcement program. The SRR stated "FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES." Facebook SUMF 100. The Data Use Policy stated that "Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data." Facebook SUMF 109. The above policies clearly disclaim control over how third-party applications operate. It is not possible for Facebook to one-hundred percent guarantee to users that no bad actor may violate Facebook's policies.

Facebook also never guaranteed how it would proceed in an enforcement investigation. The Platform Policy stated, "we *may* enforce against your app or website if we conclude that your app violates our terms or is negatively impacting the Platform" (emphasis added). Facebook SUMF 269. Instead, Facebook only outlined the potential enforcement avenues available to it, should an investigation or further action be deemed necessary. In *Illinois v. Facebook*, the Court also reached this conclusion, stating "Facebook's relevant policies only indicate the enforcement available to it and Facebook makes no guarantee as to how it will proceed in such investigations." *Illinois v. Facebook*, No. 2018 CH 03868 at 11 (March 2, 2021). A user could not have been misled about Facebook's utilization of the enforcement measures because Facebook never made guarantees of how it would proceed in such a situation. The accurate

disclosures, which dictated how Facebook *may* proceed, as a matter of law, cannot mislead users. Facebook acted in accordance with its policies, and while these enforcement actions are not what the District wanted them to be, that does not translate to a misrepresentation under the CPPA. There is also no duty imposed onto Facebook, by the CPPA or any other applicable statute, that would require Facebook to act otherwise. The District fails to plausibly plead how the application of Facebook's *discretionary* enforcement program fails to meet any statutory duty to act. The District also fails to plausibly plead a misleading representation that informed consumers that Facebook would act differently in such a scenario.

**D. Privacy Settings**

The District alleges that Facebook did not adequately explain to consumers how to change their settings regarding what information was shared with third-party applications. The District further alleges that Facebook's representations to consumers, both express and implied, that it would protect the privacy of users' personal information has a tendency to mislead consumers about a material fact. In response, Facebook asserts that the website boasted numerous resources that educated users on data sharing and how to change their settings. Facebook also contends that clear disclosures throughout their policies accurately described what data was shared and with whom.

As evidenced above, the Data Use Policy and the Statement of Rights and Responsibilities clearly set out Facebook policies and were available for users to read. Before signing up for a Facebook account, users were required to read and agree to both the Data Use Policy and the SRR. In addition to public policies that users affirmatively agreed to, users also had access to numerous tools designed to educate users on their settings and how to protect their privacy. These included the Help Center, the Privacy Tour, the Privacy Checkup, and the Privacy

Basics. Facebook SUMF 86-93. The Help Center contained educational materials, including how to navigate privacy controls. Facebook SUMF 86-88. The Privacy Tour is presented to users when creating an account. Facebook SUMF 89. The Tour walks new users through how Facebook works and how to control the sharing of their information, including with apps and websites. Facebook SUMF 89-90. The Privacy Checkup allowed users to check the scope of their information sharing, including the apps to which they had given permissions. Facebook SUMF 92. Privacy Basics provided tips and interactive guides that answer commonly asked questions on how to control user information. Facebook SUMF 93. These tools are easy to locate within the Facebook platform and possess clear interfaces where a reasonable user could readily follow along and change their settings as they please. Facebook SUMF 86-93.

Considering all of these sources of information and user-friendly tools, it is difficult to imagine what else Facebook could have conceivably done to be more forthcoming about the privacy settings. To that end, with the various policies outlined in the Data Use Policy and SRR along with the tools designed to help users configure their settings as they pleased, users were empowered to dictate the level of data that was shared with third-party applications. The privacy settings provided exactly what was promised in Facebook policies. The District has failed to plausibly plead any duty or authority that would require greater disclosures or further regulation of the privacy settings. The privacy settings and how to adjust them are not misleading.

## II. Facebook did not have a duty under CPPA to disclose alleged data misuse, such as in the Cambridge Analytica incident.

The District alleges that Facebook failed to disclose to affected consumers when their data was improperly used by third-party applications in violation of Facebook's platform policies. The District points to the Cambridge Analytica incident as a primary example. In response, Facebook asserts that they *did* notify users potentially affected by the Cambridge

Analytica data misuse. Facebook also asserts that even if Facebook had not notified users, the Cambridge Analytica incident was widely reported such that well-informed users would not have been misled by a material omission. The District's claim fails for two reasons; (1) Facebook did not have a duty to disclose the alleged data misuse to consumers, and (2) Facebook never misrepresented its actions in response to Cambridge Analytica.

A CPPA claim asks whether Facebook made material representations, omissions, or ambiguous statements that have a tendency to mislead. The CPPA never mentions or alludes to an affirmative duty to disclose data misuse. Facebook policies repeatedly disclosed the potential for data misuse by third-party applications. These disclosures negated any duty for Facebook to inform consumers when the forewarned data misuse occurred.[7] While Facebook took steps to inform consumers of the risk of data misuse and utilized various enforcement tools, a reasonable consumer had been on repeated notice that something like a Cambridge Analytica incident was possible. The District's speculation that Facebook misled consumers about data misuse fails to consider the repeated disclosures within Facebook policies.

Secondly, Facebook never misrepresented its actions in response to Cambridge Analytica.[8] In response to the first incident in December 2015, Facebook removed Kogan's app, demanded Kogan delete the user data in his possession, and began an investigation. Both Kogan and Cambridge Analytica provided written certifications that all of the data had been accounted for and destroyed. Facebook SUMF 387-391. In response to the second incident in March 2018, when Facebook learned from media inquiries that Cambridge Analytica may not have destroyed the data and may have used it for political advertising contrary to its prior representations,

[7] Indeed, at the Motions Hearing, the Court inquired about third party misuse of Facebook data by parties other than Cambridge Analytica. Counsel for the District responded that such misuse occurred on a few occasions but gave the Court the impression that such misuse was of no moment. This left the Court to wonder why the Cambridge Analytica misuse created a cause of action.

[8] See page 3-4 for a more detailed timeline of the Cambridge Analytica incident.

Facebook again took action. Facebook SUMF 392. In response, Facebook banned Cambridge Analytica and initiated an investigation. Facebook SUMF 393-394. Also, Facebook notified users who may have been affected beginning on April 9, 2018. Facebook SUMF 397-404. The notice was in the form of a dialog box upon logging into the platform, with three potential messages presented to the user, depending on whether that user had been impacted. Facebook SUMF 397-404. If a user's information was not shared, the below message was presented:

> Recently, we shared information about the potential misuse of your Facebook data by apps and websites. We also shared plans for how we're taking action to prevent this from happening in the future.
>
> Check below to see if your information may have been shared with Cambridge Analytica by the app "This is Your Digital Life."
>
> **Was My Information Shared?**
>
> Based on our available records, neither you nor your friends logged into "This Is Your Digital Life."
>
> As a result, it doesn't appear your Facebook information was shared with Cambridge Analytica by "This Is Your Digital Life."

Facebook SUMF 402.

If the user installed the app, the message included the following information as potentially shared with Cambridge Analytica:

> Your public profile, page likes, friend list, birthday and current city; Your friends public profiles, birthdays, current cities and page likes. A small number of people also shared their News Feed, timeline, posts, messages and friends hometowns with 'This is Your Digital Life.'

Facebook SUMF 403.

If the user was a non-installer friend that was potentially affected, the message included the following information as potentially shared with Cambridge Analytica:

> Your public profile, page likes, birthday and current city. A small number of people who logged into 'This is Your Digital Life' also shared their own News

> Feed, timeline, posts and messages which may have included posts and messages from you. They may also have shared your hometown information.

Facebook SUMF 404.

As the above timeline provides, Facebook took swift action in response to Cambridge Analytica. While there was no requirement to inform users of the incident, Facebook took a number of enforcement actions. First, in 2015, Facebook removed the app, demanded Kogan delete the user data in his possession, and began an investigation. Then, in 2018, Facebook banned Cambridge Analytica, began an investigation, and informed users of potential disclosure. There is no promise within Facebook's policies that dictates how Facebook should have responded differently in these situations. While the District may disagree with Facebook's approach to the situation, there is no legal basis that required Facebook to act differently. The actions that Facebook took were consistent with its stated policies. Facebook did not materially mislead consumers as to their response to Cambridge Analytica.

**Conclusion**

Upon consideration of *Facebook, Inc.'s Motion for Summary Judgment* filed on May 17, 2022*, District's Opposition to Defendant Facebook's Motion for Summary Judgment* filed on June 28, 2022, Defendant's *Reply in Support of Facebook, Inc.'s Opposed Motion for Summary Judgment* filed on July 19, 2022, the representations made by the parties during the Motion Hearing on March 21, 2023, and the entire record herein, it is this **1st** day of June 2023, hereby

**ORDERED** that *Facebook, Inc.'s Motion for Summary Judgment* is **GRANTED**; and it is further

**ORDERED**, that Plaintiff's Complaint is **DISMISSED**; and it is further

**ORDERED** that this case is now closed.

**IT IS SO ORDERED**.

Maurice A. Ross

Judge Maurice A. Ross

Copies to (via e-service):

Jimmy Rock
Jennifer Rimm
Adam Teitelbaum
J Eli Wade-Scott
*Counsel for Plaintiff*

Robert Hur
Joshua Lipshutz
Daniel Nadatowski
Alison Watkins
*Counsel for Defendant*